

ABSTRACT

A security service of computer networks having a policy builder, an LDAP-compliant database, a validator and an API. The policy builder component provides a graphical user interface to be used by a policy manager to define access policies for users seeking to access network services and resources. The graphical user interface has a grid of nodes representing access policies. The grid is arranged to correspond to a defined tree structure representing services and resources and a business relationship tree structure representing users. The graphical user interface permits the policy manager to define policy builder plug-ins for access policy customization. The LDAP-compliant database maintains the policy builder plug-ins. The validator component receives requests from users and queries the LDAP-compliant database to obtain relevant access policies as defined by the policy manager. The system provides for double inheritance of access policies such that where there is no express definition of an access policy for a node, the access policies are propagated according to the hierarchical structures of the data. The validator includes validator plug-ins for carrying out access policies corresponding to the access policies defined by policy builder plug-ins.

006T40" 54E2560